AMENDMENTS TO THE CLAIMS

1-20. **(Canceled)**

21. **(Currently Amended)** ~~The communication device of claim 19~~

A communication device for performing encrypted communication with another device, comprising:

a data generation unit operable to encrypt a first key using a public key of the other device to generate first encrypted key data, and transmit the first encrypted key data to the other device;

a decryption unit operable to receive, from the other device, second encrypted key data generated by the other device encrypting a third key using a public key of the communication device, and decrypt the second encrypted key data using a private key of the communication device to obtain a second key;

a key generation unit operable to perform a predetermined operation using the first and second keys, generate a part of a result of the predetermined operation as a first encryption key and generate another part of the result as a first hash key; and

a communication unit operable to encrypt first transmission data using the first encryption key to generate first encrypted data, apply a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed on the first encrypted data by the other device, and transmit the first encrypted data and the first detection value to the other device, wherein

said data generation unit divides an operation result obtained by applying a one-way operation to a first seed value to generate a first coefficient and a first key, generates first encrypted key data by performing encryption using the first seed value and the first coefficient based on a public key of the other device, and transmits the first encrypted key data to the other device,

said decryption unit receives, from the other device, the second encrypted key data, generates a second seed value from the second encrypted key data based on a private key of the communication device, divides an operation result obtained by applying the one-way operation to the second seed value to generate a second coefficient and a second key, checks the second encrypted key data using the second coefficient, and when the second encrypted key data is correct, outputs the second key ~~as a shared key~~ identical to a third key of the other device, and

the other device

divides an operation result obtained by applying the one-way operation to a third seed value to generate a third coefficient and [[a]]the third key, generates the second encrypted key data by performing encryption using the third seed value and the third coefficient based on a public key of the communication device, and transmits the second encrypted key data to the communication device,

receives, from the communication device, the first encrypted key data, generates a fourth seed value from the first encrypted key data based on a private key of the other device, divides an operation result obtained by applying the one-way operation to the fourth seed value to generate a fourth coefficient and a fourth key, checks the first encrypted key data using the fourth coefficient, and when the first encrypted key data is correct, outputs the fourth key ~~as a shared key~~ identical to the first key,

generates a second encryption key based on the third and fourth keys, and

performs the encrypted communication with the communication device using the second encryption key.

22-27. **(Canceled)**

28. **(Currently Amended)** The communication device of claim 21, wherein

a base element and the public key of the other device are defined in a group, the public key of the other device having been calculated by performing a power operation using the private key of the other device and the base element,

said data generation unit of the communication device divides the operation result obtained by applying the one-way operation to the first seed value which is a random number to generate the first coefficient and the first key, calculates the first element in the group by performing a power operation using the first coefficient and the base element, calculates a second element in the group by performing a power operation using the first coefficient and the public key of the other device, calculates a first verification value by performing a logical operation using the first seed value, the first element, and the second element, and outputs the first element and the first verification value as the first encrypted key data,

the other device acquires the first element and the first verification value as the first encrypted key data, calculates a third element in the group by performing a power operation using the private key of the other device and the first element, calculates a second verification value by performing the logical operation using the first verification value, the first element, and the third element, divides an operation result obtained by applying the one-way operation to the second verification value to generate a fourth efficient and a fourth key, compares an operation result of a power operation using the fourth coefficient and the base element, and the first element, and when the operation result and the first element match, recognizes the fourth key ~~as the shared key~~ identical to the first key,

the base element and the public key of the communication device are defined in the group, the public key of the communication device having been calculated by performing a power operation using the private key of the communication device and the base element,

the other device divides the operation result obtained by applying the one-way operation to the second seed value which is a random number to generate the third coefficient and the third key, calculates a fourth element in the group by performing a power operation using the third coefficient and the base element, calculates a fifth element in the group by performing a power operation using the third coefficient and the public key of the communication device, calculates a third verification value by performing the logical operation using the second seed value, the fourth element, and the fifth element, and outputs the fourth element and the third verification value as the second encrypted key data,

said decryption unit of the other device acquires the fourth element and the third verification value as the second encrypted key data, calculates a sixth element in the group by performing a power operation using the private key of the communication device and the fourth element, calculates a fourth verification value by performing the logical operation using the third verification value, the fourth element, and the sixth element, divides an operation result obtained by applying the one-way operation to the fourth verification value to generate the second efficient and the second key, compares an operation result of a power operation using the second coefficient and the base element, and the fourth element, and when the operation result and the fourth element match, recognizes the second key ~~as a shared key~~identical to the third key.

29. **(Currently Amended)** The communication device of claim 28, wherein

when P is a base point as the base element on an elliptic curve E as the group, x is the private key of the other device, $W = x*P$ is the public key of the other device, and "*" represents an operand indicating the power operation which is multiplication of a point on the elliptic curve E,

said data generation unit of the communication device

(a) generates the first seed value s_1 which is a random number;

(b) calculates a hash value $G(s_1)$ of the first seed value s;

(c) divides the hash value $G(s_1)$ to generate the first coefficient a and the first key;

(d) calculates a point $R = a*P$ as the first element and a point $Q = a*W$ as the second element, on the elliptic curve E;

(e) performs an exclusive OR using the first seed value s and a hash value obtained by applying a hash function to a result of concatenating the points R and Q to obtain the first verification value v; and

(f) outputs the point R and the first verification value v as the first encrypted key data,

the other device

(g) acquires the point R and the first verification value v;

(h) calculates point $Q' = x*R$ as the third element on the elliptic curve E;

(i) performs an exclusive OR using the first verification value v and a hash value obtained by applying a hash function to a result of concatenating the points R and Q', to obtain the second verification value s'_1;

(j) calculates a hash value $G(s'_1)$ of the second verification value s';

(k) divides the hash value $G(s'_1)$ to generate the fourth coefficient a' and the fourth key;

(l) judges whether $R = a'* P$ is established or not; and

(m) when judging that $R = a'*P$ is established, recognizes the fourth key as the shared key identical to the first key, and when P is the base point as the base element on the elliptic curve E as the group, x is the private key of the communication device, $W = x{*}P$ is the public key of the communication device,

the other device

(a) generates the third seed value s_2 which is a random number;

(b) calculates a hash value $G(s_2)$ of the third seed value s_2;

(c) divides the hash value $G(s_2)$ to generate the third coefficient a and the third key;

(d) calculates the point $R = a{*}P$ as the fourth element and the point $Q = a{*}W$ as the fifth element, on the elliptic curve E;

(e) performs an exclusive OR using the third seed value s and a hash value obtained by applying a hash function to *a* result of concatenating the points R and Q to obtain the third verification value v; and

(f) outputs the point R and the third verification value v,

the decryption unit of the communication device

(g) acquires the point R and the third verification value v;

(h) calculates the point $Q' = x{*}R$ as the sixth element on the elliptic curve E;

(i) performs an exclusive OR using the third verification value v and a hash value obtained by applying a hash function to a result of concatenating the points R and Q' to obtain the fourth verification value s'_2;

(j) calculates a hash value $G(s'_2)$ of the fourth verification value s'_2;

(k) divides the hash value $G(s'_2)$ to generate the second coefficient a' and the second key;

(l) judges whether $R = a'{*}P$ is established or not; and

(m) when judging that $R = a'{*}P$ is established, recognizes the fourth key as the shared key.

30-39. **(Canceled)**